Yokogawa Security Advisory Report

YSAR-15-0003
Published on September 10, 2015
Last updated on December 22, 2017

YSAR-15-0003: Vulnerabilities of communication functions in CENTUM and other Yokogawa products

Overview:

Vulnerabilities have been found with network communication functions in CENTUM and other Yokogawa products. Yokogawa would like customers to check this document and confirm which products are affected in order to consider security measures for the overall systems. Also please consider applying the countermeasures introduced here as needed.

Yokogawa recognizes that cyber security is one of the most important concerns in customers. Since Yokogawa will continuously strengthen cyber security on all Yokogawa products, customers are recommended to upgrade their systems for better security.

Affected Products:

The products listed that would be affected by the vulnerabilities reported in this document.
Any computer on which these products are installed has the vulnerabilities.

- CENTUM series
  - CENTUM CS 1000 (R3.08.70 or earlier)
  - CENTUM CS 3000（R3.09.50 or earlier）
  - CENTUM CS 3000 Entry（R3.09.50 or earlier）
  - CENTUM VP（R6.02.00 or earlier）
  - CENTUM VP Entry（R6.02.00 or earlier）
- ProSafe-RS (R3.02.20 or earlier)
- Exaopc（R3.73.00 or earlier）
- Exaquantum (R2.85.00 or earlier)
- Exaquantum/Batch (R2.50.30 or earlier)
- Exapilot (R3.96.10 or earlier)
- Exaplog (R3.40.00 or earlier)
- Exasmoc (R4.03.20 or earlier)
- Exarqe (R4.03.20 or earlier)
- Field Wireless Device OPC Server (R2.01.02 or earlier)
- PRM (R3.12.00 or earlier)
- STARDOM VDS (R7.30.01 or earlier)
- STARDOM OPC Server for Windows (R3.40 or earlier)
- FAST/TOOLS (R10.01 or earlier)
- B/M9000CS (R5.05.01 or earlier)
- B/M9000 VP (R7.03.04 or earlier)
- FieldMate (R1.01 or R1.02)

Overview of vulnerability:

If an intentionally crafted packet is transmitted to the process which executes control network communication, the network communication becomes unresponsive. And then the process that uses the communication function become unavailable. There is a potential risk that successful exploitation of this vulnerability allows remote attackers to execute arbitrary code.

(Reference) CVSS Base Score: 10.0, Temporal Score: 8.3

Access Vector (AV)	Local (L)	Adjacent Network (A)	Network (N)		
Access Complexity (AC)	High (H)	Medium (M)	Low (L)		
Authentication (Au)	Multiple (M)	Single (S)	None (N)		
Confidentiality Impact (C)	None (N)	Partial (P)	Complete (C)		
Integrity Impact (I)	None (N)	Partial (P)	Complete (C)		
Availability Impact (A)	None (N)	Partial (P)	Complete (C)		
Exploitability (E)	Unproven (U)	Proof-of-Concept(POC)	Functional (F)	High (H)	Not Defined (ND)
Remediation Level (RL)	Official Fix (OF)	Temporary Fix (TF)	Workaround (W)	Unavailable (U)	Not Defined (ND)
Report Confidence (RC)	Unconfirmed (UC)	Uncorroborated (UR)	Confirmed (C)	Not Defined (ND)	

When the system-wide network is properly managed (i.e., when the affected product(s) is/are on an isolated network), the risk of exploiting this vulnerability could be low.

Countermeasures:

The vulnerability will be remediated with the latest release of all the affected products, some of which are already publically available. Therefore, if the customer deems this vulnerability as a risk then we would recommend that each of the products is upgraded to the latest revision.

If it is inconvenient to upgrade to the latest versions, then it is possible to minimize the risk of this vulnerability by applying the actions outlined in the next section. Yokogawa recommends to all customers to apply an appropriate security measure to the system.

When Yokogawa service personnel perform system upgrade or install patches, those charges are borne by the customer.

Mitigation Measures:

Since the communication function containing the vulnerability is only in PCN, the vulnerability does not impact the office network (i.e. business network). It is possible to protect the PCN from an attack to this vulnerability from the external network (e.g. business network) by installing a firewall between the external network and the control system, and applying appropriate security settings. It is also recommended to manage the network appropriately so that any suspicious devices cannot be connected to the network where the affected products are connected.

Malware can also infect control systems by way of removable devices like USB sticks. Yokogawa endpoint security service is suitable to protect from the infection.

When Yokogawa service personnel perform firewall setup or install endpoint security measures, those charges are borne by the customer.

Supports and Services:

For questions related to this document or how to obtain the patch software, please contact Yokogawa service department or access the below URL for more details.
https://contact.yokogawa.com/cs/gw?c-id=000498

Reference:

1. A Complete Guide to the Common Vulnerability Scoring System Version 2.0 (CVSS)
   https://www.first.org/cvss/cvss-v2-guide.pdf
   CVSS is a common language for scoring IT vulnerabilities independent from any vendors. It provides an open framework for communicating the characteristics and impacts of IT vulnerabilities, scaling it in numeric scores.

The CVSS scores described in this document are provided “AS IS.” Yokogawa has no guarantee over the scores, and the severity caused by the vulnerabilities has to be judged by the users considering the security measures equipped with the overall systems.

Revision History:

September 10, 2015 1st Edition
March 30, 2017 2rd Edition: Update Affected Products information.
December 22, 2017 3rd Edition: URL in Supports and Services is updated.

* Contents of this document are subject to change without notice.